Patent Application of Y. Tsukamura for "Simplified Method of RSA" continued

17

[033] Abstract

A simplified signing algorithm of the RSA formula is as follows:

Sign

$$Sx = Mx \{Cx\}$$

$$= Cx^{Mx} \pmod{no}$$

Verify

Eo {Sx}
= Sx^{eo} (mod no)
=
$$Cx^{Mx*eo}$$
 (mod no)
= $Nx^{do*Mx*eo}$ (mod no)
= Nx^{Mx} (mod no)

Since
$$Nx^{do^*eo} \pmod{no} = Nx$$

where

Nx : ID # of Entity X, License # issued to Entity X

Private Key of System Authority O
Public Key of System Authority O
Modulus of the key pair Do, Eo

Cx: Secret Key of X where $Cx = Nx^{do} \pmod{no}$

Mx : Message sent by XSx : Message signed by X